0400 05-03-02

PATENT

IN THE U.S. PATENT AND TRADEMARK OFFICE

Applicant:	GEFWERT et al.	Confirmation No.:	3487
Appl. No.:	10/058,126	Group:	UNKNOWN
Filed:	January 29, 2002	Examiner:	UNKNOWN

For: METHOD AND ARRANGEMENT FOR OFFERING A SERVICE VIA INFORMATION NETWORK

L E T T E R

Assistant Commissioner for Patents
Washington, DC 20231

Date: May 8, 2002

Sir:

Under the provisions of 35 U.S.C. § 119 and 37 C.F.R. § 1.55(a), the applicant(s) hereby claim(s) the right of priority based on the following application(s):

Country	Application No.	Filed
FINLAND	20010168	January 29, 2001

A certified copy of the above-noted application(s) is(are) attached hereto.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 25-0120 for any additional fee required under 37 C.F.R. §§ 1.16 or 1.17; particularly, extension of time fees.

Respectfully submitted,

YOUNG & THOMPSON

By Benoit Castel
Benoit Castel, #35,041

745 South 23rd Street, Suite 200
Arlington, Virginia 22202
(703) 521-2297

BC/psf

Attachment

(Rev. 04/19/2000)

PATENTTI- JA REKISTERIHALLITUS
NATIONAL BOARD OF PATENTS AND REGISTRATION

Helsinki 18.3.2002

ETUOIKEUSTODISTUS
PRIORITY DOCUMENT

Hakija Applicant	**Suomen Posti Oy** **Helsinki**
Patenttihakemus nro Patent application no	**20010168**
Tekemispäivä Filing date	**29.01.2001**
Kansainvälinen luokka International class	**H04L**
Keksinnön nimitys Title of invention	**"Menetelmä ja järjestelmä palvelun tarjoamiseksi tietoverkon välityksellä"**

Täten todistetaan, että oheiset asiakirjat ovat tarkkoja jäljennöksiä patentti- ja rekisterihallitukselle alkuaan annetuista selityksestä, patenttivaatimuksista, tiivistelmästä ja piirustuksista.

This is to certify that the annexed documents are true copies of the description, claims, abstract and drawings originally filed with the Finnish Patent Office.

Pirjo Kaila
Tutkimussihteeri

Maksu 50 €
Fee 50 EUR

Maksu perustuu kauppa- ja teollisuusministeriön antamaan asetukseen 1027/2001 Patentti- ja rekisterihallituksen maksullisista suoritteista muutoksineen.

The fee is based on the Decree with amendments of the Ministry of Trade and Industry No. 1027/2001 concerning the chargeable services of the National Board of Patents and Registration of Finland.

Osoite: Arkadiankatu 6 A, P.O.Box 1160, FIN-00101 Helsinki, FINLAND
Puhelin: 09 6939 500
Telephone: + 358 9 6939 500
Telefax: 09 6939 5328
Telefax: + 358 9 6939 5328

Menetelmä ja järjestelmä palvelun tarjoamiseksi tietoverkon välityksellä – Förfarande och anordning för att bjuda service i ett datanät

Keksinnön kohteena on menetelmä ja laitteisto palvelun tarjoamiseksi tietoverkkoa käyttäen. Erityisesti keksintö koskee palvelutapahtumaan liittyvien tunnistetietojen välittämistä eri osapuolten ja -järjestelmien välillä.

Tietoverkoissa, kuten Internetissä ja matkapuhelinverkoissa uusien tuotteiden ja palvelujen tarjonta ja kysyntä on lisääntynyt voimakkaasti. Eräänä palveluna mainittakoon esimerkiksi erilaiset maksulliset viestit tai sanomat sekä palvelut ja tuotteet, joita on saatavilla useisiin erityyppisiin päätelaitteisiin käyttäjätarpeen mukaan, joita päätelaitteita voivat olla esimerkiksi PC (Personal Computer), PDA (Personal Digital Assistant), matkapuhelin ja digiTV (digitaalinen televisio). Lisäksi avoimissa verkoissa on nykyisin tarjolla entistä useammin erinäisiä verkkolomakkeita tai asiakirjoja tai sen kaltaisia palveluja, joiden käyttämiseen vaaditaan käyttäjän tunnistaminen ja todentaminen tai käyttöoikeus.

Internetissä ja vastaavissa avoimissa verkoissa tapahtuviin rekisteröitymisiin, osapuolten tunnistamiseen ja todentamiseen sekä viestien, erilaisten asiakirjojen ja dokumenttien lähettämiseen, välittämiseen ja vastaanottoon liittyvään tietoturvallisuuden parantamiseen tunnetaan erilaisia keinoja, kuten esimerkiksi käyttäjätunnuksen ja salasanan käyttö. Salasanat voivat olla kiinteitä tai vaihtuvia. Salasanat ovat usein kuitenkin hankalia muistaa niiden paljouden tai monimutkaisuuden takia, sillä lähes jokaiseen palveluun, jossa yksilön tunnistaminen tai todentaminen on välttämätöntä, on käyttäjällä oltava oma käyttäjätunnus ja salasana. Aina ei suinkaan ole mahdollista, että käyttäjän tunnus ja salasana olisivat joka järjestelmässä samoja eikä se tietoturvallisuuden kannalta ole edes järkevää. Lisäksi tunnukset ja salasanat generoidaan usein mielivaltaisiksi käytettävän järjestelmän taholta ja salasanoja täytyy yleensä vaihtaa tietyin väliajoin, jolloin salasanojen muistaminen on entistä vaikeampaa.

Ennestään tunnetaan ratkaisuja salausta vaativien palvelujen hoitamiseksi mm. US-julkaisuista 5 220 510 ja 5 870 724. Mainittujen julkaisujen mukaisissa ratkaisuissa käytetään käyttäjäkohtaisia salasanoja tai käyttäjän yksilöiviä tunnuslukuja järjestelmissä, jotka muodostavat yhteyden suoraan esimerkiksi pankin ja päätelaitteen välille tyypillisesti ATM-verkon välityksellä. Julkaisusta WO 0031608 tunnetaan myös ratkaisu, jossa kannettavan päätelaitteen tunnuslukua voidaan käyttää tunnis-

tettaessa käyttäjä hänen kytkeytyessään esimerkiksi tietokoneeseen tai järjestelmään. Lisäksi myös EP-julkaisusta 0 960 402 tunnetaan ratkaisu langattoman päätelaitteen, kuten matkapuhelimen, käytöstä pankki- ja laskunmaksupalveluissa siten, että päätelaitteessa on erillinen ns. matkapuhelinlompakko-moodi.

Tunnettujen ratkaisujen mukaisiin järjestelyihin liittyy kuitenkin eräitä epäkohtia. Ratkaisut ovat tyypillisesti tarkoitettu pelkästään tietyn pankin tai pankkipalvelun hoitamiseen. Ratkaisujen mukaisissa järjestelmissä on yleensä oma erillinen näppäimistö ja näyttö erityisesti pankkipalveluiden hoitamiseen eikä järjestelmien mukaisia laitteita yleensä voi käyttää laajemmin. Esimerkiksi tietoverkoissa käsiteltäviä lomakkeita ei yleisesti voi sähköisesti allekirjoittaa puuttuvan toimikortin ja lukijan vuoksi. Tunnetuissa menetelmissä ongelmana on lisäksi teleoperaattoreiden, palveluntuottajien ja muiden toimijoiden palveluja ja verkkoteknologioita yhdistävän tunnistamis-, todentamis- ja maksamismenetelmän puute. Verkkopalveluissa tarvitaan tehokkaita ja luotettavia maksamisen, tunnistamisen ja todentamisen menetelmiä ja rakenteita sekä järkeviä tuote-, palvelu- ja hinnoituskonsepteja. Tunnettujen ratkaisujen toimintamallit ja palvelukäytännöt eivät mahdollista järkevien ja laajaalaisten sähköisten palvelujen kehittämistä kuluttajien, yritysten ja viranomaisten tarpeisiin.

Keksinnön tavoitteena on luoda ratkaisu palvelun tarjoamiseksi siten, että edellä mainittuja tekniikan tasoon liittyviä epäkohtia voidaan vähentää. Keksintö pyrkii ratkaisemaan sen, kuinka ostotapahtumaan tai palveluun liittyvä tieto saadaan varmennettua eri osapuolten taholta ja kuinka palvelunkäyttäjät tai osapuolet voidaan tunnistaa ja todentaa yksiselitteisesti.

Keksinnön tavoitteet saavutetaan siten, että palvelunkäyttäjän päätelaitteelle lähetetään varmennuspyyntö, jonka palvelunkäyttäjä voi hyväksyä syöttämällä päätelaitteeseensa tunnuksen. Tunnus voi olla esimerkiksi nelinumeroinen tunnusluku tai vaihtoehtoisesti siinä voi olla myös kirjaimia tai erikoismerkkejä.

Keksinnön mukaiselle menetelmälle palvelun tarjoamiseksi tietoverkossa on tunnusomaista se, että siirretään avoimessa verkossa palvelutapahtumaan liittyvää tietoa, hyväksytään mainittu tieto ja suoritetaan tiedon hyväksyjän tunnistaminen suljetussa verkossa suoritettavan todentamisen avulla.

Keksinnön mukaiselle järjestelmälle palvelun tarjoamiseksi tietoverkossa on tunnusomaista se, että järjestelmä käsittää avoimen ja suljetun tietoverkon, välineet palvelutapahtumaan liittyvän tiedon siirtämiseksi avoimessa verkossa, välineet maini-

tun tiedon hyväksymiseksi ja välineet tiedon hyväksyjän tunnistamiseksi suljetussa verkossa suoritettavan todentamisen avulla.

Keksinnön eräitä edullisia suoritusmuotoja on esitetty epäitsenäisissä patenttivaatimuksissa.

Keksinnön avulla saavutetaan huomattavia etuja tekniikan tason ratkaisuihin verrattuna. Keksinnön mukainen menetelmä mahdollistaa palvelunkäyttäjän tunnistamisen ja vahvan todentamisen esimerkiksi käyttäjän päätelaitteen, kuten matkapuhelimen, avulla. Keksinnön avulla voidaan mm. avoimessa tietoverkossa tarjottavaan palveluun tai tapahtumaan liittyviä tietoja tai varmistuspyyntöjä lähettää luotettavasti suljetussa verkossa olevaan palvelunkäyttäjän päätelaitteeseen varmistusta, käyttäjän identifioimista tai tietojen hyväksymistä varten.

Lisäksi keksinnön avulla on mahdollista suorittaa luotettavasti tapahtumaan liittyvien molempien osapuolten tunnistaminen, siirrettävien asiakirjojen tai dokumenttien oikeaksi todistaminen ja alkuperän varmistaminen, tietojen luottamuksellisuuden ja eheyden varmistaminen, tapahtuman tai toimenpiteen kiistämättömyys sekä tapahtuma-ajankohdan rekisteröinti.

Keksinnön avulla voidaan hoitaa myös notaaripalveluja, kuten aikaleimoja ja arkistointia. Notaaripalveluja vaaditaan mm. sähköisten viestien ja sanomien, virallisten tai virallisluonteisten asiakirjojen ja dokumenttien toimittamisessa, jakelussa ja säilyttämisessä. Näitä toimintoja varten tarvitaan tietoverkkomaailmassa ns. kolmas luotettava osapuoli (KLO), joka on riippumaton kaikista muista palveluketjuun kuuluvista osapuolista tai sähköisten lomakkeiden lähettäjistä ja vastaanottajista. KLO voi sijaita tietyssä kohtaa palveluketjua palvelutapahtumaan liittyvien osapuolten välissä, jossa se tarjoaa roolinsa mukaisia varmennuspalveluita, kuten osapuolten tunnistamista ja todentamista.

Tässä patenttihakemuksessa käytetään mm. seuraavia käsitteitä:

- "Asiakas" on keksinnön mukaisen menetelmän käyttäjä ja kauppatapahtuman osapuoli, joka hankkii tai ostaa tuotteen tai palvelun esimerkiksi perinteisesti myyjältä tai vaihtoehtoisesti tietoverkossa tai sen kautta.

- "Avoimen verkon palveluntuottaja" voi olla esimerkiksi Internet-operaattori, joka tuottaa tietoverkkopalveluita. Lisäksi avoimen verkon palveluntuottaja voi tarjota sähköisiä verkkolomakkeita esimerkiksi tietoverkkojen välityksellä

sekä toimia osapuolten tunnistajana ja osapuolten välisenä tietojen välittäjänä.

- "Avoimen verkon päätelaite" voi olla esimerkiksi sopivilla muistiyksiköillä, tietoliikenneyhteydellä ja prosessorilla varustettu tietokone tai työasema, PDA, matkapuhelin, digiTV tai vastaava järjestelmä. Avoimen verkon päätelaite voi olla yhteydessä avoimen verkon palveluntuottajan järjestelmään joko suoraan avoimen verkon välityksellä tai vaihtoehtoisesti suljetun verkon välityksellä esimerkiksi jos päätelaite on kytketty langattomaan päätelaitteeseen, kuten matkapuhelimeen.

- "Digitaalinen allekirjoitus" perustuu ns. julkisen avaimen menetelmään, jolla tunnistetaan ja todennetaan viestin lähettäjä ja vastaanottaja, taataan toimenpiteen kiistämättömyys sekä varmistetaan tietojen luottamuksellisuus ja eheys.

- "Kolmas luotettava osapuoli" yhdistää palvelun tuottajan ja käyttäjän tarjoamalla roolinsa mukaisia varmennuspalveluita, kuten osapuolten tunnistaminen ja todentaminen.

- "Lähettäjä" lähettää viestin tai sanoman sähköisessä muodossa vastaanottajalle.

- "Myyjä" on keksinnön mukaisen menetelmän käyttäjä, joka myy esimerkiksi tuotetta tai palvelua joko perinteisesti kauppapaikallaan tai vaihtoehtoisesti tietoverkossa tai sen kautta.

- "Palvelunkäyttäjä" on esimerkiksi asiakas, myyjä, yksityinen kuluttaja tai kansalainen, yritys tai yhteisö, viranomainen tai julkishallinto, joka käyttää keksinnön mukaista menetelmää tai mainittuja palveluntuottajan palveluja.

- "Sanoma, pyyntö tai viesti" voi käsittää sähköisessä muodossa esimerkiksi yleisen tunnisteen tai tunnisteosan, vastaanottajan nimen tai verkko- tai hakemisto-osoitteen, verkkopalvelun tuottajan nimen ja osoitteen sekä sähköpostiosoitteen. Lisäksi se voi olla esimerkiksi kokonainen asiakirja tai dokumentti, sähköpostiviesti liitetiedostoineen, itsenäinen julkaisu, tuote tai palvelu, tiedote tai tiedonanto, huomautus tai muistutus, hälytys tai virheilmoitus, palvelu- tai tarjouspyyntö, kehote tai opaste, ilmoitus tai mainos, lupa tai haaste. Kaikille näille on yhteistä se, että ne on toimitettu, julkaistu tai välitetty vastaanottajalle sähköisessä muodossa.

- "Suljetun verkon palveluntuottaja" voi olla esimerkiksi matkapuhelinoperaattori, joka välittää viestejä ja sanomia tai tietoja esimerkiksi Internet- ja langattomissa verkoissa ja voi toimia osapuolten tunnistajana ja osapuolten välisenä tietojen välittäjänä.

- "Suljetun verkon päätelaite" voi olla esimerkiksi PDA, matkapuhelin tai vastaavan kaltainen laite. Erityisesti päätelaite voi olla langattomassa verkossa toimiva matkapuhelin, joka on varustettu sopivalla SIM-kortilla (Subscriber Identity Module).

- "Sähköinen lomake" on jollakin sähköisellä välineellä tuotettu, välitetty tai jaettu, näytetty tai täytetty määrämuotoinen lomake, joka usein on kopio alkuperäisestä paperilomakkeesta.

- "Todentaminen" varmistaa järjestelmän käyttäjän tunnistamisen oikeellisuuden.

- "Tunnistaminen" on tapahtuma, jossa käyttäjä kertoo järjestelmälle identiteettinsä eli tunnistetiedot. Tunnistetiedot voidaan vaihtoehtoisesti lukea myös käyttäjän lähettämästä viestistä tai sanomasta.

- "Varmennus tai varmenne" sisältää osapuolten tai palvelun tunnistetiedot, viittauksen käyttöoikeuksiin, viestien tai sanomien salausavaimet ja digitaalisen allekirjoituksen vaatimat salaiset avaimet ja varmenteen myöntäneen tahon eli liikkeellelaskijan tiedot.

- "Vastaanottaja" ottaa hänelle sähköisesti lähetetyn viestin tai sanoman vastaan.

- "Verkkolomakkeella" tarkoitettaan kehittynyttä älykästä sähköistä lomaketta, jossa määrämuotoisuuden lisäksi on toiminnallisia ominaisuuksia, kuten esitäyttö, opasteet ja liittymä sovellukseen tai suoraan tietokantaan, eikä sillä yleensä ole yksi yhteen vastinetta tai suhdetta paperilomakkeeseen. Verkkolomaketta on myös mahdollista verrata perinteiseen sovelluksen näyttöön. Yhtenä älykkään lomakkeen kriteerinä voidaan myös pitää tietojen haku- tai täyttömahdollisuutta sekä digitaalista allekirjoitusta.

Tarkastellaan ensimmäisenä esimerkkinä avoimessa verkossa tapahtuvaan palvelu- tai kauppatapahtumaan liittyvien tapahtumatietojen välittämistä osapuolten välillä. Osapuolia eli palvelukäyttäjiä tässä tapauksessa ovat myyjä ja asiakas. Esimerkissä

myyjäosapuoli tarjoaa kauppapaikallaan tuotteitaan tai palveluaan. Asiakas kerää ostoksensa ostoskoriin, josta myyjä siirtää kauppatapahtuman tiedot omaan kassa- ja laskutusjärjestelmään. Maksutapahtumassa kauppatapahtuman tiedot lähetetään myyjän laskutusjärjestelmästä tietoverkon, kuten Internetin välityksellä palveluntuottajan tai operaattorin järjestelmään ja sieltä edelleen langattoman suljetun verkon välityksellä asiakkaan päätelaitteelle.

Asiakas tunnistetaan ja todennetaan palveluntuottajan avulla, minkä jälkeen voidaan aloittaa kauppatapahtumatietojen käsittely asiakkaan päätelaitteella niin, että asiakas voi varmistua saapuneiden tietojen, kuten loppusumman ja ajankohdan, oikeellisuudesta ja että ne liittyvät juuri hänen kauppatapahtumaansa.

Jos asiakas hyväksyy hänen päätelaitteelle lähetetyt palveluun tai kauppatapahtumaan liittyvät tiedot, kuten esimerkiksi laskun, voidaan maksaminen suorittaa antamalla päätelaitteelle tunnus, joka voi olla esimerkiksi matkapuhelimen tapauksessa matkapuhelimen PIN-luku (Personal Indentification Number). Vastaavasti myyjä saa tiedon asiakkaan maksusuorituksesta tietoverkkojen välityksellä kassa- tai laskutusjärjestelmäänsä.

Seuraavaksi tarkastellaan esimerkkinä tietoverkoissa, kuten Internetissä tarjottavaa sähköistä asiointipalvelua. Tässä esimerkissä palvelunkäyttäjä voi olla esimerkiksi yksityinen käyttäjä, jolla on käytössään avoimen verkon päätelaite, kuten tietokone tai työasema, ja suljetun verkon päätelaite, kuten matkapuhelin. Esimerkissä selaimella noudetaan sähköisiä lomakkeita palveluntuottajan palvelimelta palvelunkäyttäjän työasemalle toimenpiteitä, kuten tietojen hakua, täyttämistä tai allekirjoittamista varten. Viimeistelty lomake voidaan allekirjoittaa digitaalisesti työasemasta riippumattoman ja fyysisesti erillään olevan langattoman päätelaitteen avulla ja lähettää avoimessa verkossa vastaanottajalle.

Jos sähköinen lomake päätetään allekirjoittaa digitaalisesti ennen lähetystä, palvelunkäyttäjä lähettää allekirjoituspyynnön palveluntuottajalle. Allekirjoituspyyntö voidaan lähettää joko palvelunkäyttäjän työasemalta tai langattomalta päätelaitteelta. Tämän jälkeen palveluntuottaja tyypillisesti vahvistaa ja välittää allekirjoituspyynnön palvelunkäyttäjän langattomaan päätelaitteeseen tunnistettuaan ja todennettuaan avoimessa ja suljetussa verkossa olevat päätelaitteet. Allekirjoitus voidaan suorittaa digitaalisesti antamalla suljetussa verkossa olevalle palvelunkäyttäjän päätelaitteelle tunnus. Digitaalinen allekirjoitus toimitetaan palvelunkäyttäjien tunnistajana ja todentajana toimivan palveluntuottajan välityksellä palvelunkäyttäjän työasemalle,

jossa palvelunkäyttäjä voi liittää sen digitaalisesti allekirjoitettavaan lomakkeeseensa tai muuten suorittaa asianmukaiset toimenpiteet.

Edellä mainittu suljetussa verkossa toimiva asiakkaan tai palvelunkäyttäjän päätelaite on tyypillisesti PDA, matkapuhelin tai vastaavan kaltainen järjestelmä, jolla voidaan hyväksyä vastaanotettu pyyntö tai varmenne esimerkiksi näppäilemällä tietty tunnus. Erityisesti päätelaite voi olla langattomassa verkossa toimiva matkapuhelin, joka on varustettu sopivalla SIM-kortilla (Subscriber Identity Module). Päätelaitteessa voi lisäksi olla prosessori sekä tietty salausavain, joka voi olla sijoitettu esimerkiksi laitteen SIM-korttiin.

Edellä mainittu avoimessa verkossa toimiva palvelunkäyttäjän tai myyjän päätelaite voi olla esimerkiksi sopivilla muistiyksiköillä, tietoliikenneyhteydellä ja prosessorilla varustettu tietokone tai työasema, PDA, matkapuhelin, digiTV tai vastaava järjestelmä, jolla voidaan lähettää ja vastaanottaa edellä mainitun kaltainen pyyntö, varmenne tai palvelu.

Edellä mainituissa esimerkeissä tietoverkossa tapahtuvalle sähköiselle asioinnille asetetaan tiettyjä perusvaatimuksia, kuten osapuolten tunnistaminen ja todentaminen, tapahtuman ja toimenpiteen kiistämättömyys ja ajankohdan rekisteröitävyys, tietojen luottamuksellisuuden ja eheyden varmistaminen, asiakirjan oikeaksi todistaminen ja alkuperän varmistaminen sekä notaaripalvelut, kuten aikaleima ja arkistointi. Lisäksi voidaan vaatia välitettävän tiedon salaus käyttämällä määrättyjä salausalgoritmeja. Tiedon salaus ja salauksen purkaminen voidaan edullisesti suorittaa esimerkiksi suljetussa verkossa olevan palvelunkäyttäjän päätelaitteen, päätelaitteessa olevaan SIM-korttiin tallennetun salausavaimen ja päätelaitteessa mahdollisesti olevan prosessorin avulla.

Seuraavassa osiossa selostetaan keksinnön eräitä edullisia suoritusmuotoja hieman tarkemmin viitaten oheisiin kuviin, joissa

kuva 1 esittää vuokaaviona erästä suoritusmuotoa palveluun liittyvän varmennuksen hyväksymiseksi keksinnön mukaisesti,

kuva 2 esittää erästä keksinnön mukaista järjestelmää tuotteen tai palvelun maksamiseksi,

kuva 3 esittää erästä keksinnön mukaista järjestelmää lomakkeen digitaaliseksi allekirjoittamiseksi,

kuva 4 esittää vuokaaviona erästä menetelmää tuotteen tai palvelun maksamiseksi keksinnön mukaisesti, ja

kuva 5 esittää vuokaaviona erästä menetelmää lomakkeen digitaaliseksi allekirjoittamiseksi keksinnön mukaisesti.

Kuva 1 esittää vuokaaviona erästä suoritusmuotoa keksinnön keskeisestä ideasta tarjottavaan palveluun liittyvän varmennuksen hyväksymiseksi. Tarjottava palvelu on tyypillisesti kauppatapahtuma tai ostosuoritus, mutta palvelu voi olla myös sähköisen lomakkeen digitaalinen allekirjoittaminen, palveluun rekisteröityminen tai muu vastaava palvelu, jossa vaaditaan palvelunkäyttäjän luotettavaa tunnistamista ja todentamista. Keksinnön idean mukaisesti voidaan suorittaa luotettavasti myös tapahtumaan liittyvien molempien osapuolten tunnistaminen, siirrettävien asiakirjojen tai dokumenttien oikeaksi todistaminen ja alkuperän varmistaminen, tietojen luottamuksellisuuden ja eheyden varmistaminen, tapahtuman tai toimenpiteen kiistämättömyys, tapahtuma-ajankohdan rekisteröinti sekä aineiston arkistointi.

Tässä esimerkissä palvelunkäyttäjiä ovat myyjä, jolla on avoimessa verkossa oleva päätelaite ja asiakas, jolla on suljetussa verkossa oleva päätelaite. Myyjä voi lisäksi olla myös luonteeltaan palveluntarjoaja, joka tarjoaa palveluita avoimessa verkossa.

Palvelua voidaan tarjota 101 ja käyttää esimerkiksi tyypillisessä kauppaympäristössä, jolloin avoimen verkon palvelunkäyttäjä eli myyjä voi siirtää tapahtumatiedot suljetun verkon palvelunkäyttäjän eli asiakkaan päätelaitteeseen eri tietoverkkojen välityksellä. Palvelu voi olla vaihtoehtoisesti myös tietoverkossa tarjottavaa palvelua, kuten esimerkiksi ns. verkkokauppaa, jolloin tapahtumatietojen välittäminen asiakkaan päätelaitteeseen voidaan suorittaa automaattisesti. Jos asiakas käyttää esimerkiksi palvelua, jossa vaaditaan käyttäjän tunnistamista tai palveluun liittyvien tietojen varmistamista käyttäjän taholta, voidaan vaiheessa 102 lähettää asiakkaalle varmennuspyyntö esimerkiksi tämän suljetun verkon päätelaitteelle avoimen ja suljetun verkon sekä näiden verkkojen palveluntuottajien avulla. Varmennuspyyntö voi sisältää palvelutapahtumaan liittyvää tietoa tai sillä voidaan varmistua asiakkaan henkilöllisyydestä ja siten mahdollisesti myös tämän oikeuksista tarjottavaan palveluun. Vaiheessa 103 voidaan tunnistaa varmennuspyynnön lähettäjä ja/tai vastaanottaja esimerkiksi avoimen tai suljetun tai molempien verkkojen palveluntuottajien avulla.

Pyyntö voidaan lähettää esimerkiksi avoimessa verkossa olevalla myyjän päätelaitteella, kuten tietokoneella, jolloin pyyntö edullisesti lähetetään ensin avoimen ver-

kon palveluita toimittavalle palveluntuottajalle, joka voi tunnistaa ja todentaa pyynnön lähettäneen osapuolen. Avoimen verkon palveluntuottaja voi välittää pyynnön edullisesti suljetun verkon palveluntuottajalle, kuten esimerkiksi matkapuhelinoperaattorille, joka puolestaan voi tunnistaa ja todentaa pyynnönsaajan eli asiakkaan päätelaitteen. Suljetun verkon palveluntuottaja voi tämän jälkeen välittää pyynnön asiakkaan päätelaitteelle.

Saatuaan varmennuspyynnön pyynnönsaaja eli asiakas voi tarkistaa pyynnössä olevat tiedot ja joko hyväksyä pyynnön tai kieltäytyä hyväksymästä sitä. Jos asiakas päättää hyväksyä pyynnön, voidaan hyväksyminen suorittaa vaiheessa 104 syöttämällä suljetun verkon päätelaitteeseen tunnus. Annettava tunnus on edullisesti päätelaitteen PIN-luku, mutta se voi olla myös jokin muu käyttäjäkohtainen tunnusluku. Tunnus todennetaan vaiheessa 105 esimerkiksi päätelaitteen SIM-kortin avulla. Vaiheessa 106 hyväksytty varmennus lähetetään myyjälle. Lähetetty varmennus välitetään edullisesti esimerkiksi suljetun tai avoimen verkon palveluntuottajan tai vaihtoehtoisesti molempien avulla, jotka voivat tunnistaa asiakkaan tai molemmat osapuolet vaiheessa 107 ja välittää varmennuksen edelleen myyjälle. Saatuaan hyväksyvän varmennuksen, myyjä voi antaa asiakkaalle esimerkiksi oikeuden palvelun tai tuotteen käyttöön. Asiakkaan päätelaitteellaan hyväksymä pyyntö tai varmenne voidaan välittää vastaavaa tietoliikennelinkkiä pitkin takaisin myyjälle, kuin mitä linkkiä pitkin pyyntö välitettiin myyjältä asiakkaan päätelaitteelle. Tällöin asiakkaan ja myyjän tunnistaminen ja todentaminen voidaan suorittaa luotettavasti esimerkiksi suljetun ja avoimen verkon palveluntuottajien avulla.

Välitettävän tiedon virallisuudesta tai tärkeydestä riippuen tieto voidaan toimittaa vaihtoehtoisesti myös tietoverkoissa notaaripalveluja tarjoavan kolmannen luotettavan osapuolen (KLO) välityksellä. KLO voi sijaita määrätyssä kohtaa palveluketjua palvelutapahtumaan liittyvien osapuolten välissä. Notaaripalveluja tai KLO:n toimintoja ei tämän hakemuksen yhteydessä kuvata tai määritellä tarkemmin.

Kuva 2 esittää keksinnön erään suoritusmuodon mukaista järjestelmää 200 maksusuoritukseen tai muuhun kauppatapahtumaan tai palveluun liittyvän tiedon hyväksymiseksi asiakkaan 223 päätelaitteella 207. Suoritusmuodon mukaisessa menetelmässä myyjä 224 siirtää kauppatapahtumaan liittyvän tiedon kassa- ja laskutusjärjestelmäänsä 201, josta tapahtumatiedot lähetetään avoimen verkon 202, kuten Internetin (I) välityksellä palveluntuottajan järjestelmään 203 vaiheessa 1.0. Avoin verkko voi vaihtoehtoisesti olla myös jokin muu tiedonsiirtämiseen tarkoitettu ratkaisu. Tapahtumatiedot voivat sisältää tietoa esimerkiksi tapahtuma-ajasta, myyjästä 224,

tuotteesta, ostajasta tai asiakkaasta 223 sekä tunnisteen, jolla asiakas 223 tunnistetaan. Tunniste voi olla esimerkiksi viitteellinen asiakastunnus.

Avoimen verkon palveluntuottaja 203 voi tunnistaa myyjän 224 tai asiakkaan 223 saadessaan tapahtumatiedot myyjän järjestelmästä ja välittää 204 tiedot edelleen suljetun verkon palveluntuottajalle 205, joka lähettää tiedot edelleen asiakkaan 223 päätelaitteelle 207 suljetun verkon 206 välityksellä vaiheessa 1.1. Myös suljetun verkon palveluntuottaja 205 voi tässä vaiheessa tunnistaa myyjän 224 sekä asiakkaan 223 ja tämän langattoman päätelaitteen 207. Palveluntuottaja 205 on tyypillisesti esimerkiksi langattoman verkon verkko-operaattori, kuten matkapuhelinoperaattori, joka välittää viestejä ja sanomia tai tietoja langattomissa verkoissa. Palveluntuottaja 205 voi välittää tietoa myös Internetissä Langaton verkko 206 voi olla esimerkiksi matkapuhelinverkko.

Kauppatapahtumatietojen käsittely voidaan suorittaa asiakkaan 223 päätelaitteella 207 tyypillisesti siten, että asiakas voi varmistua saapuneiden tietojen oikeellisuudesta, kuten loppusummasta, tapahtuma-ajasta ja siitä, että tiedot liittyvät hänen kauppatapahtumaansa. Kauppatapahtumatietojen hyväksyminen, kuten maksaminen, voidaan suorittaa asiakkaan 223 päätelaitteella 207 antamalla päätelaitteelle esimerkiksi edellä mainitun tyyppinen tunnus. Tunnuksen antamisen jälkeen kauppatapahtuman hyväksymiseen liittyvä tieto voidaan lähettää suljetun verkon palveluntuottajalle 205 suljetun verkon 206 välityksellä vaiheessa 2.0, joka palveluntuottaja välittää 204 tiedon edelleen avoimen verkon palveluntuottajalle 203. Myyjä 224 saa tiedon asiakkaan maksusuorituksesta omaan järjestelmäänsä 201 palveluntuottajalta 203 avoimen verkon 202 välityksellä vaiheessa 2.1.

Myös kauppatapahtuman hyväksymiseen liittyvän tiedon välitysvaiheessa sekä suljetun verkon palveluntuottaja 205 että avoimen verkon palveluntuottaja 203 voivat tunnistaa asiakkaan 223 tai tämän päätelaitteen 207 sekä myyjän 224 tai tämän järjestelmän 201. Lisäksi kauppatapahtumaan liittyvät tiedot voidaan välittää kolmannen luotettavan osapuolen välityksellä, joka voi luotettavasti tunnistaa tapahtuman osapuolet.

Myyjän 224 kassa- ja laskutusjärjestelmässä 201 on tyypillisesti välineet 208 palvelutapahtumaan liittyvän tiedon lähettämiseksi avoimen tai suljetun verkon palveluntuottajalle sekä välineet 219 palvelutapahtuman hyväksymiseen liittyvän tiedon vastaanottamiseksi. Avoimen verkon palveluntuottajan järjestelmässä 203 on yleensä välineet 209 palvelutapahtumaan liittyvän tiedon lähettäjän tunnistamiseksi sekä välineet 217 palvelutapahtuman hyväksymiseen liittyvän tiedon vastaanottajan tun-

nistamiseksi ja välineet 218 palvelutapahtuman hyväksymiseen liittyvän tiedon siirtämiseksi myyjän 224 järjestelmään 201.

Suljetun verkon palveluntarjoajan järjestelmässä 205 on tyypillisesti välineet 210 palvelutapahtumaan liittyvän tiedon vastaanottajan tunnistamiseksi, välineet 211 palvelutapahtumaan liittyvän tiedon siirtämiseksi asiakkaan päätelaitteelle 207 sekä välineet 216 palvelutapahtuman hyväksymiseen liittyvän tiedon lähettäjän tunnistamiseksi. Asiakkaan 223 päätelaitteessa 207 on yleensä välineet 212 palvelutapahtumaan liittyvän tiedon vastaanottamiseksi, välineet 213 palvelutapahtumaan liittyvän tiedon hyväksymiseksi, välineet 214 päätelaitteella 207 annetun tunnuksen tunnistamiseksi, välineet 215 palvelutapahtumaan liittyvän tiedon siirtämiseksi suljetun verkon palveluntuottajalle 205 tai avoimen verkon palveluntuottajalle 203, prosessori 222 sekä SIM-kortti 220, jossa SIM-kortissa on edullisesti tallennettuna salausavain 221 tiedon salaamiseksi ja salauksen purkamiseksi.

Lisäksi suljetun verkon palveluntuottajan 205 ja avoimen verkon palveluntuottajan 203 järjestelmissä on välineet tiedonsiirtämiseksi toistensa välillä esimerkiksi tiedonsiirtoon tarkoitetun järjestelmän 204 avulla. Lisäksi palveluntuottajien 203, 205 järjestelmissä voi olla keskenään samoja välineitä, jolloin tietojen välittäminen myyjän 224 päätelaitteen 201 ja asiakkaan 223 päätelaitteen 207 välillä voidaan hoitaa joko vaihtoehtoisesti vain suljetun verkon tai vain avoimen verkon palveluntuottajan välityksellä.

Kuva 3 esittää erästä keksinnön mukaista järjestelmää 300 avoimessa verkossa 202 tarjottavan sähköisen asiointipalvelun käyttämiseksi, jossa menetelmässä noudetaan sähköisiä verkkolomakkeita palveluntuottajan palvelimelta 203 palvelunkäyttäjän 223 päätelaitteelle 301, kuten työasemalle tai tietokoneelle, avoimen tietoverkon 202, kuten Internetin (I) välityksellä vaiheessa 1.0. Verkkolomakkeet voidaan noutaa päätelaitteelle 301 esimerkiksi toimenpiteitä, kuten tietojen hakua, täyttämistä tai digitaalista allekirjoittamista varten. Lomakkeiden nouto voi tapahtua esimerkiksi päätelaitteessa 301 olevan selaimen avulla tai lomakkeet voidaan vaihtoehtoisesti toimittaa myös muilla tavoin, kuten esimerkiksi levykkeellä, sähköpostitse tai muulla vastaavalla tiedonsiirtoon ja -välittämiseen tarkoitetulla menetelmällä. Lisäksi palvelunkäyttäjä 223 voi itse tuottaa käsiteltävänä olevan lomakkeen omalla päätelaitteellaan 301. Esimerkin mukainen palveluntuottaja 203 on tyypillisesti tietty yritys, yhteisö, viranomainen tai julkishallinto ja erityisesti palveluntuottaja voi olla Internet-operaattori, joka tuottaa tietoverkkopalveluja ja välittää tietoa esimerkiksi avoimessa verkossa olevan palvelunkäyttäjän 223 päätelaitteen 301, kuten työase-

man tai tietokoneen, ja suljetussa verkossa olevan palvelunkäyttäjän 223 päätelaitteen 207, kuten matkapuhelimen, välillä.

Palveluntuottaja 203 saa tyypillisesti kuittauksen lomakkeen vastaanotosta palvelunkäyttäjältä 223, joka käyttäjä voi esimerkiksi muokata, allekirjoittaa, lähettää tai arkistoida sähköisen lomakkeen tai asiakirjan. Jos palvelunkäyttäjä 223 haluaa allekirjoittaa sähköisen lomakkeen, voi hän lähettää päätelaitteellaan 301 allekirjoituspyynnön tai -sanoman palveluntuottajalle 203 avoimen tietoverkon 202 välityksellä vaiheessa 2.0. Allekirjoituspyyntö voidaan lähettää myös palvelunkäyttäjän 223 suljetun verkon päätelaitteelta 207. Avoimen verkon palveluntuottaja 203 voi tässä vaiheessa tunnistaa palvelunkäyttäjän 223 päätelaitteen 301 (tai 207) ja välittää 204 allekirjoituspyynnön edelleen suljetun verkon palveluntuottajalle 205, joka voi jatkolähettää pyynnön esimerkiksi palvelunkäyttäjän langattomaan päätelaitteeseen 207 suljetun langattoman verkon 206 välityksellä vaiheessa 2.1. Myös suljetun verkon palveluntuottaja 205 voi tässä vaiheessa tunnistaa palvelunkäyttäjän ja tämän langattoman päätelaitteen 207.

Palvelunkäyttäjä 223 voi halutessaan allekirjoittaa päätelaitteella 207 vastaanottamansa sanoman digitaalisesti esimerkiksi suljetun verkon päätelaitteen ja tunnuksen avulla. Tunnus voi olla esimerkiksi edellä mainitun tapainen tunnusluku. Tunnuksen antamisen jälkeen sanoma voidaan allekirjoittaa ja lähettää suljetun langattoman verkon 206 välityksellä suljetun verkon palveluntuottajalle 205 vaiheessa 3.0. Sanoma voidaan salata esimerkiksi päätelaitteen SIM-korttiin 220 tallennetun salausavaimen 221 ja päätelaitteessa olevan prosessorin 222 avulla. Palveluntuottaja 205 voi tunnistaa palvelunkäyttäjän 223 suljetun verkon päätelaitteen 207 ja välittää 204 allekirjoitetun sanoman avoimen verkon palveluntuottajalle 203, joka välittää sanoman edelleen palvelunkäyttäjän 223 avoimen verkon päätelaitteelle 301 avoimen verkon 202 välityksellä vaiheessa 3.1.

Palvelunkäyttäjän 223 päätelaite 301 voi olla esimerkiksi sopivilla muistiyksiköillä, tietoliikenneyhteydellä ja prosessorilla varustettu työasema tai tietokone, PDA, matkapuhelin, digiTV tai vastaava järjestelmä, jolla voidaan vastaanottaa edellä mainitun kaltainen verkkolomake sekä lähettää allekirjoituspyyntö ja vastaanottaa allekirjoitettu sanoma. Palvelunkäyttäjän päätelaitteessa 301 on tyypillisesti välineet 302 lomakkeen hakemiseksi, vastaanottamiseksi ja käsittelemiseksi sekä välineet 303 allekirjoituspyynnön lähettämiseksi ja allekirjoituksen vastaanottamiseksi.

Palvelunkäyttäjän 223 suljetussa verkossa toimiva päätelaite 207 on tyypillisesti PDA, matkapuhelin tai vastaavan kaltainen järjestelmä, jolla voidaan hyväksyä vas-

taanotettu allekirjoituspyyntö esimerkiksi näppäilemällä tietty tunnus tai tunnusluku. Erityisesti päätelaite 207 voi olla langattomassa verkossa toimiva matkapuhelin, joka on varustettu sopivalla SIM-kortilla 220, SIM-korttiin tallennetulla salausavaimella 221 sekä lisäksi mahdollisesti myös prosessorilla 222. Prosessori mahdollistaa mm. sähköisen allekirjoituksen käytön sekä matkapuhelimen avulla tehtävän ja salauksen vaatiman laskutoimituksen suorittamisen.

Lisäksi avoimen ja suljetun verkon palveluntuottajien järjestelmissä voi olla keskenään samoja välineitä osapuolten tunnistamiseksi ja tiedon välittämiseksi, jolloin tietojen välittäminen palvelunkäyttäjän 223 avoimen verkon päätelaitteen 301 ja suljetun verkon päätelaitteen 207 välillä voidaan hoitaa joko vaihtoehtoisesti vain avoimen tai vain suljetun verkon palveluntuottajan välityksellä. Tapahtumaan liittyvien osapuolten tunnistaminen palveluntuottajien avulla suoritetaan edullisesti aina välitettäessä tapahtumaan liittyvää tietoa. Tieto voidaan vaihtoehtoisesti välittää myös kolmannen luotettavan osapuolen välityksellä, jolloin tietojen eheys sekä muut vastaavat tietoturvallisuuteen, tiedon varmistamiseen ja osapuolten luotettavaan tunnistamiseen liittyvät toimenpiteet voidaan suorittaa mainitun kolmannen luotettavan osapuolen avulla.

Kuva 4 esittää vuokaaviona erästä keksinnön mukaista menetelmää tuotteen tai palvelun maksamiseksi 401. Vaiheessa 402 asiakas ostaa tuotteen ja vaiheessa 403 myyjä siirtää asiakkaan kauppatapahtumatiedot kassa- ja laskutusjärjestelmäänsä, joka on yhteydessä esimerkiksi avoimeen tietoverkkoon, kuten Internet-tietoverkkoon. Vaiheessa 404 myyjän laskutusjärjestelmästä välitetään kauppatapahtumatiedot tyypillisesti Internet-tietoverkon välityksellä avoimen verkon palveluntuottajan järjestelmään. Palveluntuottaja voi olla esimerkiksi tietoverkon verkko-operaattori, joka tarjoaa tietoverkko- tai Internet-palveluita ja jonka kanssa myyjä on mahdollisesti tehnyt palvelusopimuksen. Avoimen verkon palveluntuottaja voi tässä vaiheessa tunnistaa myyjän ja välittää kauppatapahtumatiedot edelleen suljetun verkon palveluntuottajalle vaiheessa 405. Suljetun verkon palveluntuottaja voi olla esimerkiksi langattoman verkon verkko-operaattori, joka puolestaan voi tunnistaa langattomassa verkossa olevan asiakkaan päätelaitteen ja välittää kauppatapahtumatiedot edelleen päätelaitteelle vaiheessa 406. Vaihtoehtoisesti myös avoimen verkon palveluntuottaja voi tunnistaa asiakkaan ja välittää tapahtumatiedot suoraan asiakkaan päätelaitteelle vaiheessa 406.

Asiakkaan saadessa kauppatapahtumatiedot suljetun verkon päätelaitteelleen hän voi varmistua kauppatapahtumatietojen oikeellisuudesta vaiheessa 407. Kauppatapahtumatiedot voidaan myös salata esimerkiksi jollain salausalgoritmilla, jolloin vai-

heessa 407 suoritetaan myös salauksen purku ja tapahtumatietojen esittäminen selkokielisesti. Vaiheessa 408 asiakas voi valita, hyväksyykö hän tapahtumatiedot vai ei. Tuotteen tai palvelun maksaminen keskeytetään vaiheessa 409, jos asiakas ei hyväksy tapahtumatietoja. Jos asiakas hyväksyy tiedot, suoritetaan maksaminen vaiheessa 410 antamalla suljetun verkon päätelaitteelle esimerkiksi edellä mainitun kaltainen tunnus.

Vaiheessa 411 asiakkaan antama tunnus todennetaan esimerkiksi vertaamalla annettua tunnusta päätelaitteen SIM-kortin tietoihin. Jos annettu tunnus on oikein, lähetetään tieto maksun suorittamisesta vaiheessa 413 suljetun verkon palveluntuottajalle. Maksutieto voidaan lähettää myös suoraan avoimen verkon palveluntarjoajalle vaiheessa 412. Lähetettävä tieto voidaan myös salata ennen lähetystä esimerkiksi suljetun verkon päätelaitteen SIM-kortille tallennetun salausavaimen ja päätelaitteessa mahdollisesti olevan prosessorin avulla.

Suljetun verkon palveluntuottaja voi tunnistaa suljetun verkon päätelaitteen ja päätelaitteen käyttäjän vaiheen 413 yhteydessä ja välittää tiedon edelleen avoimen verkon palveluntuottajan järjestelmään vaiheessa 412. Avoimen verkon palveluntuottaja voi tunnistaa kauppatapahtumaan liittyvän myyjän vaiheen 412 yhteydessä ja välittää tiedon maksusuorituksesta edelleen myyjän laskutusjärjestelmään vaiheessa 414. Vaihtoehtoisesti tietojen välittäminen tapahtuman eri osapuolten välillä voidaan toteuttaa joko yksistään vain suljetun tai vain avoimen verkon palveluntuottajan avulla, jolloin molemmat tietojen välittäjät (palveluntuottajat) voivat tunnistaa molemmat tapahtuman osapuolet.

Kuva 5 esittää vuokaaviona erästä keksinnön mukaista menetelmää lomakkeen digitaaliseksi allekirjoittamiseksi 501. Vaiheessa 502 sähköistä verkkolomaketta voidaan tarjota esimerkiksi tietoverkossa, josta se voidaan vaiheessa 503 noutaa palvelunkäyttäjän avoimen verkon päätelaitteelle, kuten esimerkiksi tietokoneelle tai muulle vastaavalle laitteelle, jatkotoimenpiteitä varten. Lomake voidaan toimittaa myös muilla tavoin tai se voidaan vaihtoehtoisesti luoda myös palvelunkäyttäjän avoimen verkon päätelaitteella. Jos lomake on toimitettu palveluntuottajan järjestelmästä palvelunkäyttäjän avoimen verkon päätelaitteelle esimerkiksi tietoverkon välityksellä, voidaan vaiheessa 504 lähettää palveluntuottajalle kuittaus lomakkeen vastaanottamisesta ja vastaanottamisen onnistumisesta.

Lisäksi vaiheiden 502 ja 503 aikana voidaan suorittaa osapuolten tunnistaminen, jos haettava verkkolomake sitä vaatii. Tällainen verkkolomake voi olla esimerkiksi verotoimistosta tai vastaavasta paikasta lähetettävä ko. palvelunkäyttäjän tiedoilla varus-

tettu lomake, joka toimitetaan tietoturvasyistä johtuen vain asianomaiselle palvelunkäyttäjälle. Tällöin palvelunkäyttäjälle voidaan lähettää tämän päätelaitteelle allekirjoitus- tai varmennuspyyntö tässä selostuksessa esitettyjen suoritusmuotojen mukaisesti, jolloin voidaan varmistua palvelunkäyttäjän identiteetistä ja oikeuksista mainitun lomakkeen noutamiseen tietoverkon avulla.

Palvelunkäyttäjä voi tehdä saamalleen lomakkeelle erilaisia toimenpiteitä, kuten esimerkiksi muokata, lähettää, arkistoida tai allekirjoittaa sen. Vaiheessa 505 voidaan päättää, allekirjoitetaanko lomake vai ei. Vaiheessa 506 suoritusmuodon mukainen menetelmä lopetetaan, jos lomake päätetään olla allekirjoittamatta. Jos lomake puolestaan päätetään allekirjoittaa, voidaan avoimen verkon palveluntuottajalle lähettää allekirjoituspyyntö vaiheessa 507. Vaiheessa 507 avoimen verkon palveluntuottaja voi myös tunnistaa allekirjoitustapahtumaan liittyvät osapuolet. Allekirjoituspyyntö voidaan lähettää palvelunkäyttäjän avoimen verkon päätelaitteella tai vaihtoehtoisesti myös palvelunkäyttäjän suljetun verkon päätelaitteella. Avoimen verkon palveluntuottaja voi välittää allekirjoituspyynnön edelleen suljetun verkon palveluntuottajalle vaiheessa 508, jolloin suljetun verkon palveluntuottaja voi tunnistaa palvelunkäyttäjän suljetun verkon päätelaitteen ja jatkolähettää pyynnön edelleen päätelaitteelle vaiheessa 509. Vaihtoehtoisesti myös avoimen verkon palveluntuottaja voi tunnistaa palvelunkäyttäjän suljetun verkon päätelaitteen ja jatkolähettää allekirjoituspyynnön suoraan palvelunkäyttäjän suljetun verkon päätelaitteelle vaiheessa 509.

Saatuaan allekirjoituspyynnön suljetun verkon päätelaitteelleen palvelunkäyttäjä voi allekirjoittaa pyynnön antamalla tunnuksen päätelaitteelle vaiheessa 510. Tunnus voi olla esimerkiksi edellä mainitun tyyppinen tunnusluku. Vaiheessa 511 käyttäjän antama tunnus todennetaan. Allekirjoitus voidaan haluttaessa myös salata tunnuksen antamisen jälkeen esimerkiksi päätelaitteen SIM-kortille tallennetun salausavaimen ja päätelaitteessa mahdollisesti olevan prosessorin avulla. Allekirjoitus voidaan lähettää suljetun verkon palveluntuottajalle 205 vaiheessa 513, jolloin palveluntuottaja voi tunnistaa palvelunkäyttäjän suljetun verkon päätelaitteen ja välittää allekirjoituksen edelleen avoimen verkon palveluntuottajalle 203 vaiheessa 512. Allekirjoitus voidaan lähettää käyttäjän suljetun verkon päätelaitteelta 207 vaihtoehtoisesti myös suoraan avoimen verkon palveluntuottajalle 203 vaiheessa 512, jolloin avoimen verkon palveluntuottaja voi tunnistaa käyttäjän suljetun verkon päätelaitteen 207. Avoimen verkon palveluntuottaja voi tunnistaa tyypillisesti myös palvelunkäyttäjän avoimen verkon päätelaitteen 301 ja välittää allekirjoituksen edelleen päätelaitteelle 301 vaiheessa 514.

Edellä on esitetty vain eräitä keksinnön mukaisen ratkaisun suoritusmuotoja. Keksinnön mukaista periaatetta voidaan luonnollisesti muunnella patenttivaatimusten määrittelemän suoja-alueen puitteissa esimerkiksi toteutuksen yksityiskohtien sekä käyttöalueiden osalta. Erityisesti käytettävät päätelaitteet voivat olla minkä tahansa tyyppisiä järjestelmiä, joiden avulla keksinnön mukaista ideaa voidaan käyttää tai soveltaa. Lisäksi avoimen ja suljetun verkon palveluntuottajien menetelmät ja järjestelmät voivat olla joissain tapauksissa samoja, jolloin esimerkiksi lomakkeen haku tai allekirjoituspyyntö voidaan suorittaa tai välittää vaihtoehtoisesti kumman palveluntuottajan avulla tahansa.

Patenttivaatimukset

1. Menetelmä (101) palvelun tarjoamiseksi tietoverkossa, **tunnettu** siitä, että siirretään (102) avoimessa verkossa palvelutapahtumaan liittyvää tietoa, hyväksytään (104) mainittu tieto ja suoritetaan tiedon hyväksyjän tunnistaminen (107) suljetussa verkossa suoritettavan todentamisen avulla.

2 Patenttivaatimuksen 1 mukainen menetelmä, **tunnettu** siitä, että mainittu tiedon hyväksyminen käsittää vaiheet, joissa

- suoritetaan (104) mainittuun palvelutapahtumaan liittyvän tiedon hyväksyminen syöttämällä suljetun verkon päätelaitteelle (207) tunnus,
- tunnistetaan ja todennetaan (105) mainittu päätelaitteelle syötetty tunnus, ja
- siirretään (412, 413) mainittu palvelutapahtuman hyväksymiseen liittyvä tieto palveluntuottajalle (203, 205) suljetun verkon avulla.

3. Patenttivaatimuksen 1 mukainen menetelmä, **tunnettu** siitä, että mainittu palvelutapahtuma on kauppatapahtuma (401).

4. Patenttivaatimuksen 1 mukainen menetelmä, **tunnettu** siitä, että mainittu palvelutapahtuma on lomakkeen digitaalinen allekirjoittaminen (501).

5. Patenttivaatimuksen 1 mukainen menetelmä, **tunnettu** siitä, että tiedon siirtämiseen liittyvät osapuolet tunnistetaan palveluntuottajan (203, 205) avulla.

6. Patenttivaatimuksen 1 mukainen menetelmä, **tunnettu** siitä, että tiedon siirtämiseen liittyvät osapuolet tunnistetaan kolmannen luotettavan osapuolen avulla.

7. Patenttivaatimuksen 1 mukainen menetelmä, **tunnettu** siitä, että mainittu päätelaitteella (207) annettava tunnus on SIM-kortilla (220) todennettavissa oleva PIN-luku.

8. Patenttivaatimuksen 1 mukainen menetelmä, **tunnettu** siitä, että mainittuun palvelutapahtumaan liittyvän tiedon salauksen purkaminen suoritetaan palvelunkäyttäjän päätelaitteen (207) avulla.

9. Patenttivaatimuksen 1 mukainen menetelmä, **tunnettu** siitä, että mainitun palvelutapahtuman hyväksymiseen liittyvä tieto salataan palvelunkäyttäjän päätelaitteen avulla (207).

10. Patenttivaatimuksen 1 mukainen menetelmä, **tunnettu** siitä, että mainitut palvelutapahtumatiedot lähetetään palvelunkäyttäjän järjestelmästä (201, 301) palveluntuottajan (203, 205) järjestelmään avoimen tietoverkon (202) välityksellä.

11. Patenttivaatimuksen 1 mukainen menetelmä, **tunnettu** siitä, että mainitun palvelutapahtuman hyväksymiseen liittyvä tieto lähetetään palveluntuottajan (203, 205) järjestelmään suljetun verkon (206) välityksellä.

12. Järjestelmä (200, 300) palvelun tarjoamiseksi tietoverkossa, **tunnettu** siitä, että järjestelmä käsittää avoimen (202) ja suljetun (206) tietoverkon, välineet (208. 303) palvelutapahtumaan liittyvän tiedon siirtämiseksi avoimessa verkossa, välineet (213) mainitun tiedon hyväksymiseksi ja välineet (216) tiedon hyväksyjän tunnistamiseksi suljetussa verkossa suoritettavan todentamisen avulla.

13 Patenttivaatimuksen 12 mukainen järjestelmä, **tunnettu** siitä, että mainittu tiedon hyväksyminen käsittää lisäksi

- välineet (213) mainittuun palvelutapahtumaan liittyvän tiedon hyväksymiseksi syöttämällä suljetun verkon päätelaitteelle (207) tunnus,

- välineet (214) mainitun päätelaitteelle syötetyn tunnuksen tunnistamiseksi ja todentamiseksi, ja

- välineet (215) mainitun palvelutapahtuman hyväksymiseen liittyvän tiedon siirtämiseksi palveluntuottajalle (203, 205) suljetun verkon (206) avulla.

14. Patenttivaatimuksen 12 mukainen järjestelmä, **tunnettu** siitä, että mainittu suljettu verkko (206) on matkapuhelinverkko.

15. Patenttivaatimuksen 12 mukainen järjestelmä, **tunnettu** siitä, että mainittu avoin verkko (202) on Internet-tietoverkko.

16. Patenttivaatimuksen 13 mukainen järjestelmä, **tunnettu** siitä, että mainittu suljetun verkon päätelaite (207) on langaton päätelaite.

17. Patenttivaatimuksen 16 mukainen järjestelmä, **tunnettu** siitä, että mainitussa päätelaitteessa (207) on SIM-kortti (220).

18. Patenttivaatimuksen 16 mukainen järjestelmä, **tunnettu** siitä, että mainitun päätelaitteen (207) SIM-kortissa (220) on tallennettuna salausavain (221).

19. Patenttivaatimuksen 16 mukainen järjestelmä, **tunnettu** siitä, että mainitussa päätelaitteessa (207) on prosessori (222) tiedon salaamiseksi ja salauksen purkamiseksi.

(57) Tiivistelmä

Keksinnön kohteena on menetelmä ja järjestelmä (300) palvelun tarjoamiseksi avointa (202) ja suljettua (206) verkkoa käyttäen. Erityisesti keksintö koskee palvelutapahtumaan liittyvien tunnistetietojen välittämistä eri osapuolten ja -järjestelmien välillä. Keksinnön eräänä ajatuksena on se, että palvelutapahtumaan liittyvää tietoa siirretään palvelunkäyttäjän 223 suljetun verkon päätelaitteelle (207) palvelun hyväksymistä tai palvelunkäyttäjän identifioimista varten. Palvelun hyväksyminen tai käyttäjän tunnistaminen on mahdollista suorittaa antamalla palvelunkäyttäjän päätelaitteella (207) tunnus. Lisäksi keksinnön eräänä ajatuksena on palvelutapahtuman osapuolten (223, 224) luotettava tunnistaminen ja todentaminen palveluntuottajan (203, 205) tai kolmannen luotettavan osapuolen avulla.

Fig. 2

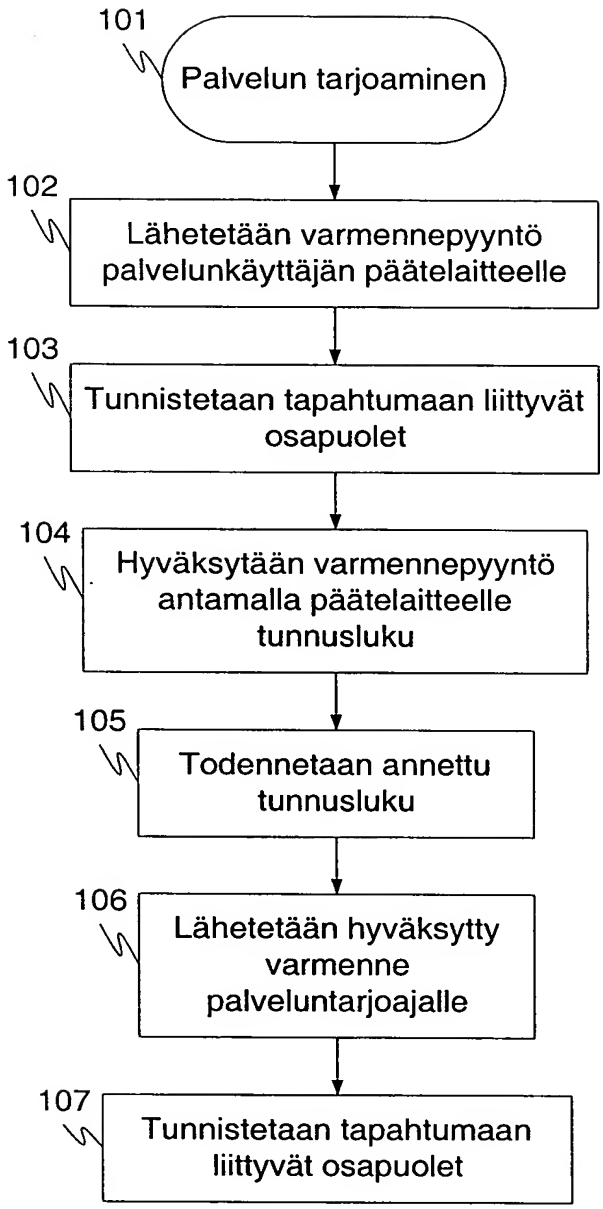
101
Palvelun tarjoaminen
102
Lähetetään varmennepyyntö palvelunkäyttäjän päätelaitteelle
103
Tunnistetaan tapahtumaan liittyvät osapuolet
104
Hyväksytään varmennepyyntö antamalla päätelaitteelle tunnusluku
105
Todennetaan annettu tunnusluku
106
Lähetetään hyväksytty varmenne palveluntarjoajalle
107
Tunnistetaan tapahtumaan liittyvät osapuolet

FIG. 1

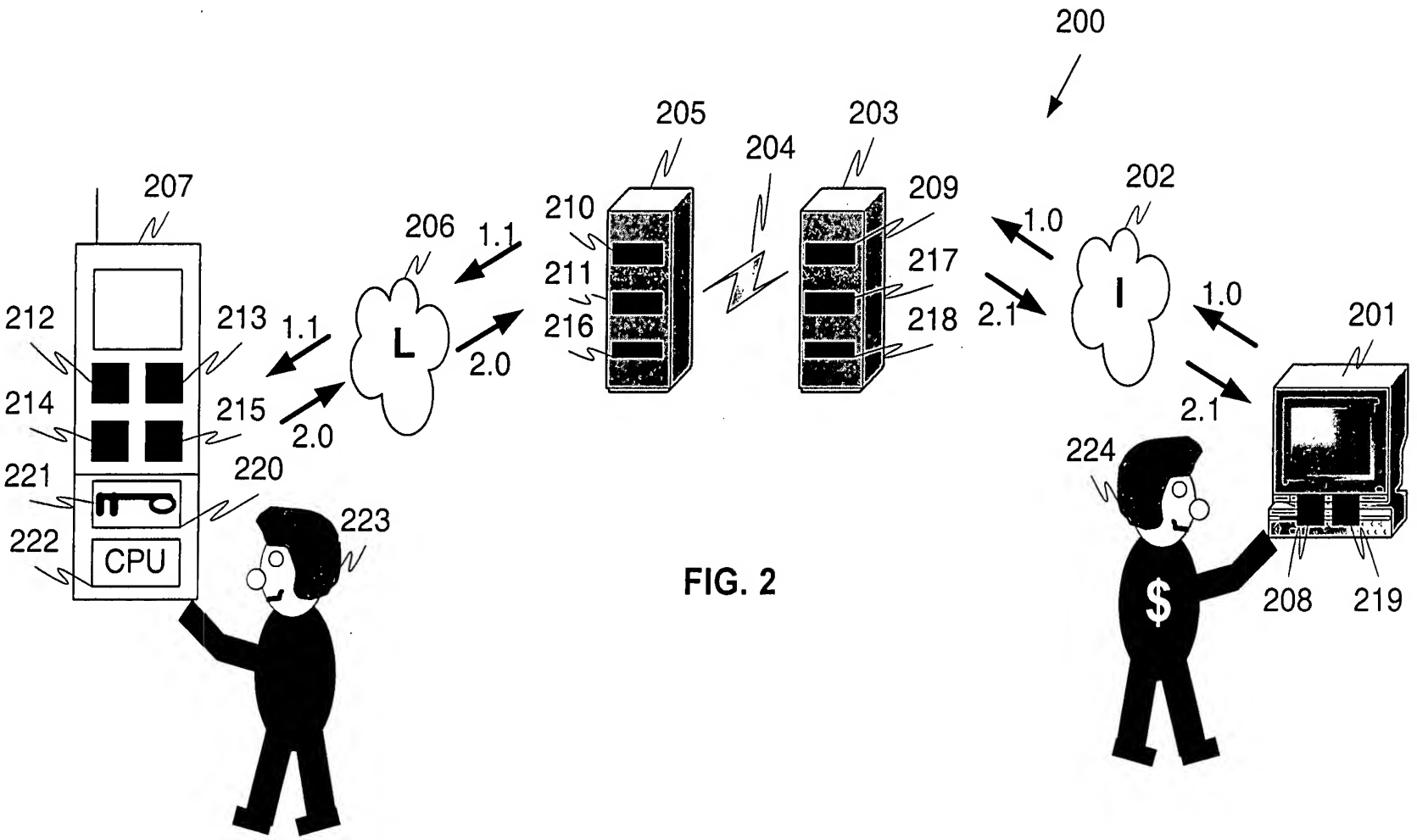

FIG. 2

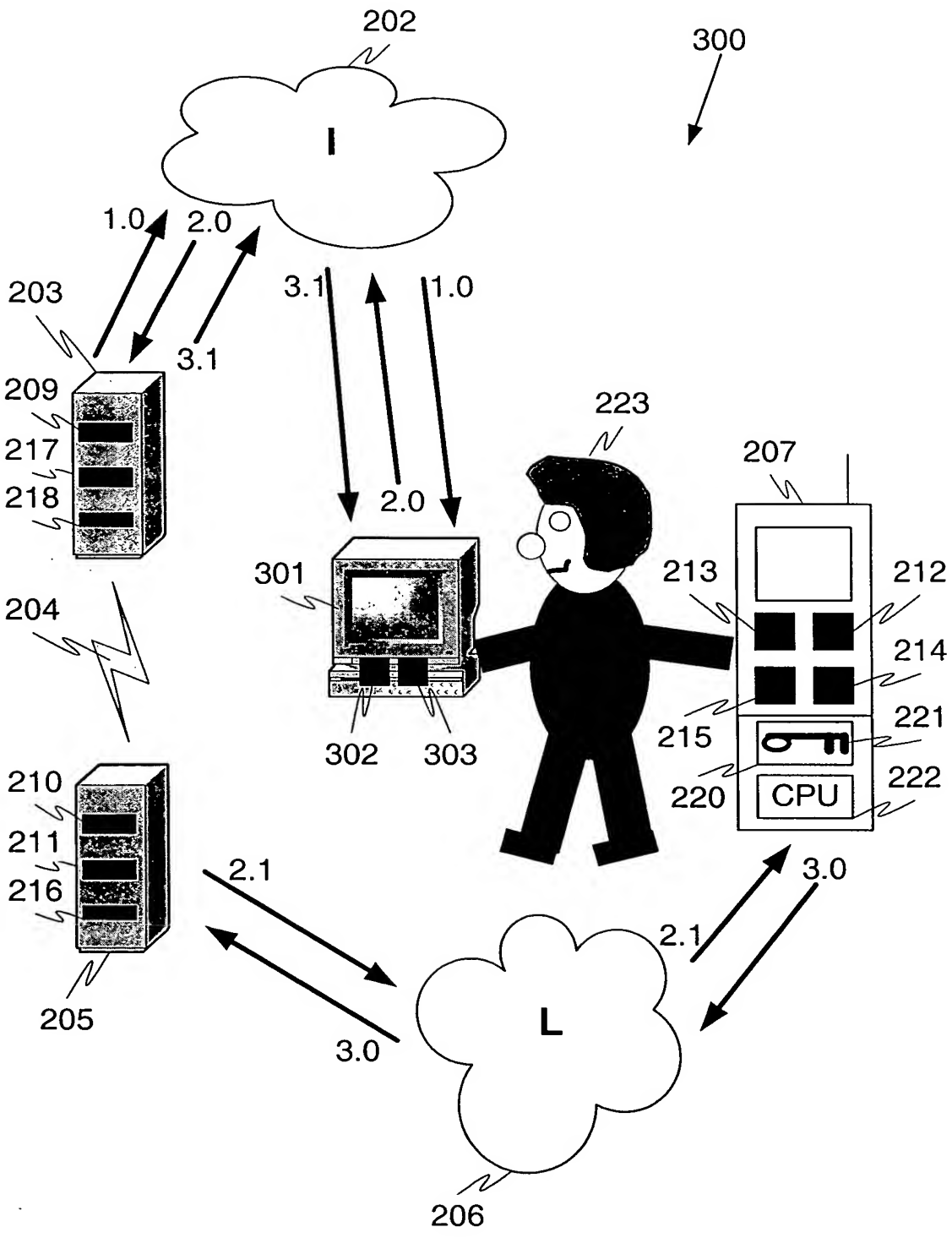
202
300
I
1.0
2.0
3.1
203
3.1
1.0
209
217
218
223
207
2.0
301
213
212
214
204
215
221
302
303
220
CPU
222
210
211
216
2.1
3.0
2.1
205
3.0
L
206

FIG. 3

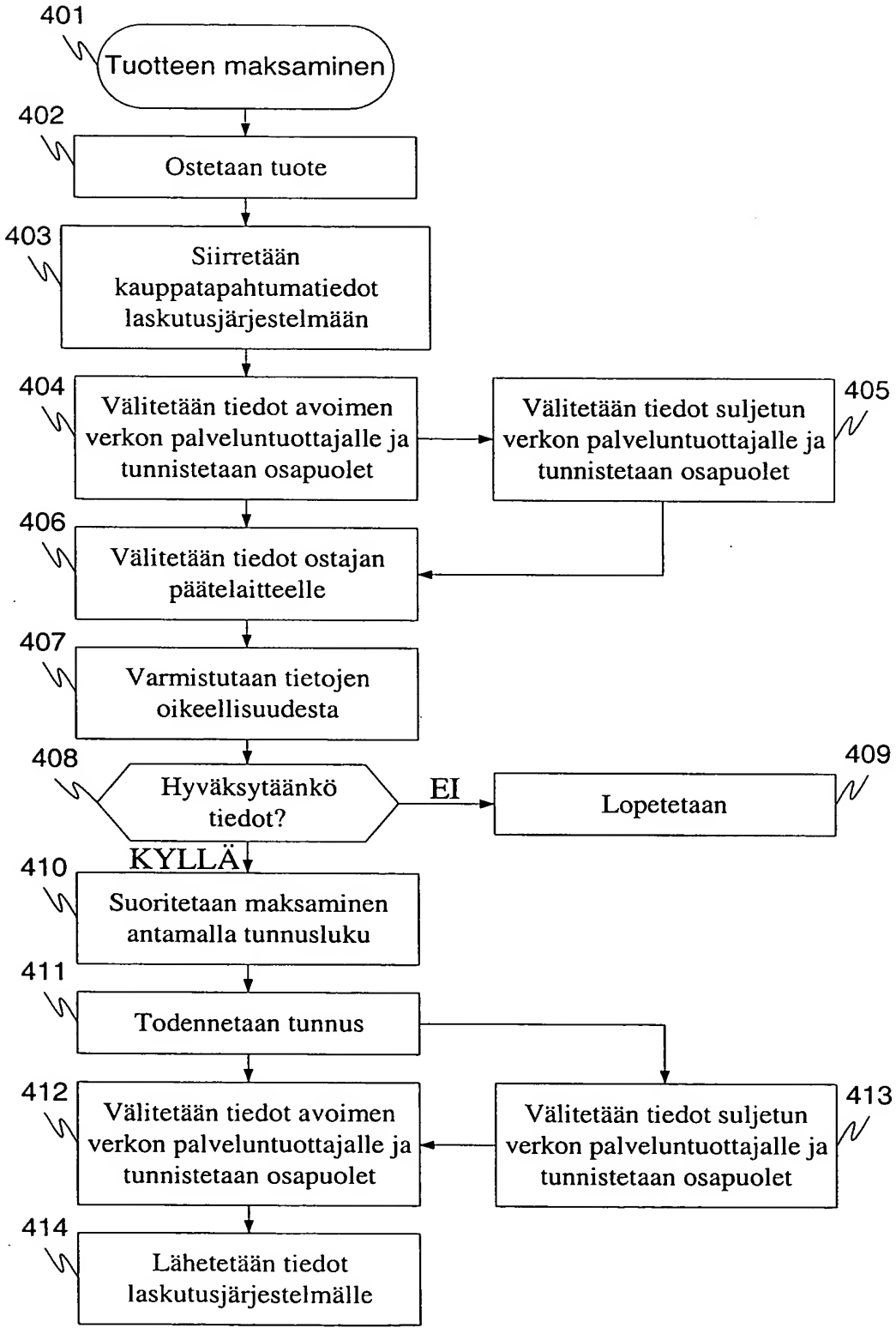
401
Tuotteen maksaminen
402
Ostetaan tuote
403
Siirretään kauppatapahtumatiedot laskutusjärjestelmään
404
Välitetään tiedot avoimen verkon palveluntuottajalle ja tunnistetaan osapuolet
405
Välitetään tiedot suljetun verkon palveluntuottajalle ja tunnistetaan osapuolet
406
Välitetään tiedot ostajan päätelaitteelle
407
Varmistutaan tietojen oikeellisuudesta
408
Hyväksytäänkö tiedot?
EI
409
Lopetetaan
KYLLÄ
410
Suoritetaan maksaminen antamalla tunnusluku
411
Todennetaan tunnus
412
Välitetään tiedot avoimen verkon palveluntuottajalle ja tunnistetaan osapuolet
413
Välitetään tiedot suljetun verkon palveluntuottajalle ja tunnistetaan osapuolet
414
Lähetetään tiedot laskutusjärjestelmälle

FIG. 4

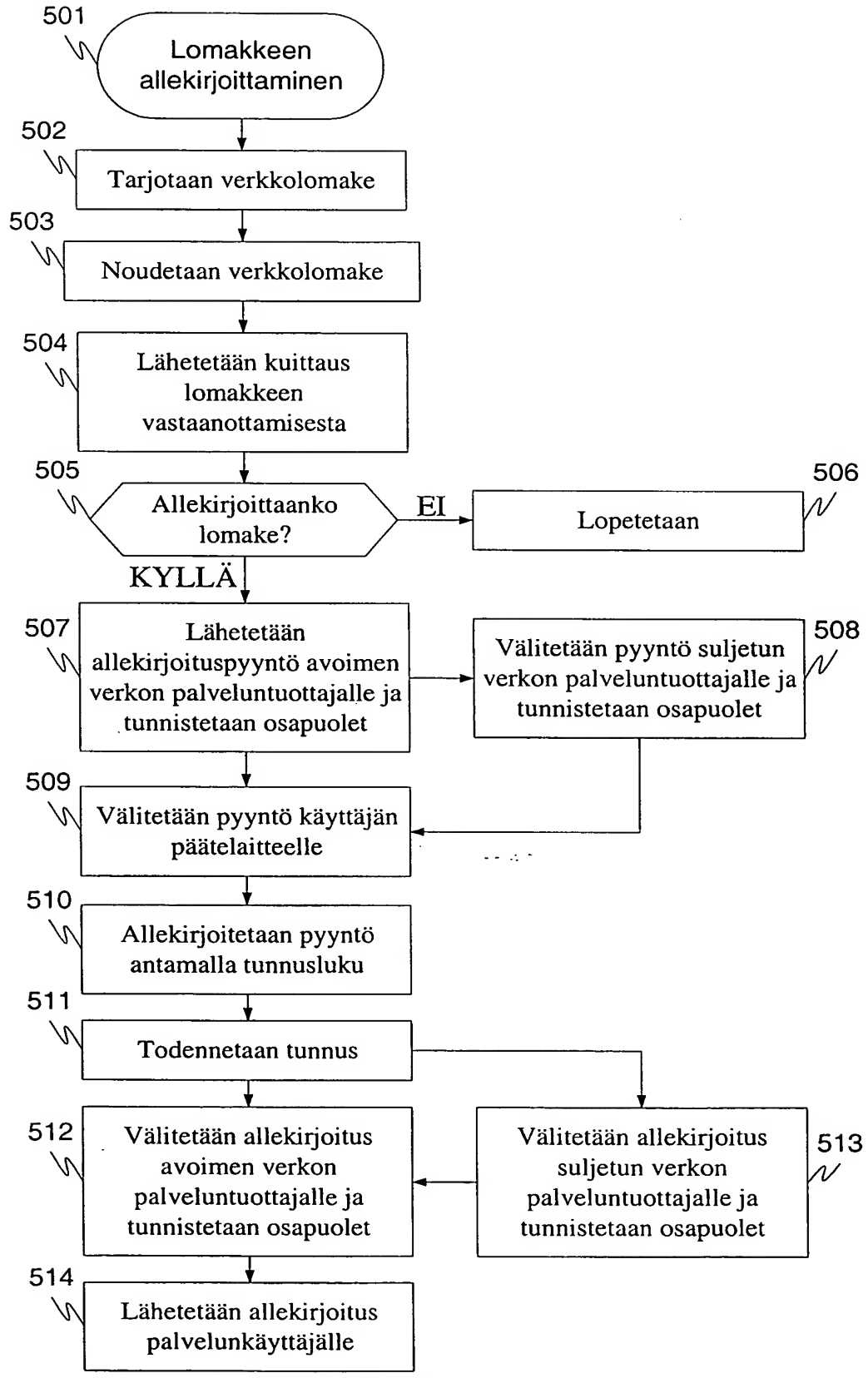
501
Lomakkeen allekirjoittaminen
502
Tarjotaan verkkolomake
503
Noudetaan verkkolomake
504
Lähetetään kuittaus lomakkeen vastaanottamisesta
505
Allekirjoittaanko lomake?
EI
506
Lopetetaan
KYLLÄ
507
Lähetetään allekirjoituspyyntö avoimen verkon palveluntuottajalle ja tunnistetaan osapuolet
508
Välitetään pyyntö suljetun verkon palveluntuottajalle ja tunnistetaan osapuolet
509
Välitetään pyyntö käyttäjän päätelaitteelle
510
Allekirjoitetaan pyyntö antamalla tunnusluku
511
Todennetaan tunnus
512
Välitetään allekirjoitus avoimen verkon palveluntuottajalle ja tunnistetaan osapuolet
513
Välitetään allekirjoitus suljetun verkon palveluntuottajalle ja tunnistetaan osapuolet
514
Lähetetään allekirjoitus palvelunkäyttäjälle

FIG. 5